June 16, 2021

VIA U.S. 1ST CLASS MAIL & EMAIL

Office of the Attorney General
Consumer Protection and Antitrust
Gateway Professional Center
600 E. Boulevard Ave. Dept. 125
Bismarck, ND 58505
Email: ndag@nd.gov

Re: Notice of Data Security Incident

Dear Sir or Madam:

Our office represents North Iowa Area Community College ("NIACC") located at 500 College Drive, Mason City, Iowa 50401. Pursuant to N.D.C.C. § 51-30-02, we are writing to notify your office of an event that may affect some personal information, as defined in N.D.C.C. § 51-30-01 (4), relating to one (1) North Dakota resident. The investigation into this matter is ongoing, and this notice may be supplemented with any new significant facts learned after its submission.

Nature of the Data Event

On Tuesday, May 18, 2021, an unknown and unauthorized individual impersonated a NIACC employee and sent a phishing email to another NIACC employee requesting student information. This phishing attack led to the compromise of two documents containing student information and account balances. Within 30 minutes after the incident, the NIACC employee discovered they were a victim of a phishing attack. The NIACC employee immediately reported the incident to NIACC Administration. NIACC Administration contacted the school's Chief Information Officer immediately.

Within 24 hours, NIACC notified all potentially affected students by email about this incident. The text of this email is attached as ***Exhibit A***. NIACC also notified all faculty and staff with a summary of the incident. NIACC Administration also reported the incident to the Mason City Police Department and the Federal Bureau of Investigation.

The document in this data security incident related to the North Dakota resident we are notifying your office about included the following information: name, address, student identification number, social security number, cell phone number, home phone number, and student account balance. No other information was contained in this compromised document.

Notice to North Dakota Resident

On June 15, 2021, NIACC mailed written notices of this incident to all potentially affected individuals, which includes the one (1) North Dakota resident. We have enclosed an anonymized version of the letter here as ***Exhibit B***. In addition, NIACC mailed a notice to another North Dakota resident about whom less information was exposed in the incident. This information

does not constitute "Personal Information" as defined N.D.C.C. § 51-30-01, but NIACC opted to provide notification to this individual as a courtesy.

Other Steps Taken and To Be Taken

In addition to alerting students about the incident, NIACC has provided students with guidance to help them stay vigilant about protecting their information and incidents of fraud. NIACC recommended students review their account statements, monitor free credit reports, and report any suspicious activity or suspected incidence of identity theft to proper law enforcement authorities, including the Attorney General's office and the Federal Trade Commission (FTC). NIACC provided the contact information for the three national credit reporting agencies and informed students of their right to place a "security freeze" on their credit reports. NIACC also recommended that students contact the NIACC Business Office to securely pay their tuition, housing fees, and student fees.

NIACC is also offering all potentially affected students with identity theft protection services through ID Experts®. The services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. NIACC has encouraged affected individuals to enroll and take full advantage of these services.

To help prevent this type of incident in the future, additional cybersecurity training has been required to help all faculty and staff identify and report future phishing emails. NIACC is also taking further remedial steps to strengthen its policies and procedures to ensure faculty and staff verify all requests for protected information and that they do not share this information absent appropriate encryption.

Contact Information

NIACC takes the privacy and security of its students' information seriously and is committed to protecting their information. Should your office have any questions regarding this notification or other aspects of the data security event, please contact us at (515) 242-2400.

Sincerely,

Brian McCormac

Enclosures

EXHIBIT A

Dear NIACC Students,

NIACC has learned that criminals may contact you demanding immediate payment of tuition and fees owed to NIACC. They may try to prove that they are legitimate by providing you with personal identifying information, including student account numbers. They may impersonate NIACC, lenders, or state or federal agencies. You may have already been contacted within the last 24 hours. Only pay tuition, housing fees and student fees through NIACC's business office or through TrojanHome. DO NOT send money to anyone else purporting to be collecting monies owed to the college who calls, texts, or emails you. NIACC wants to protect its students and is investigating this fraud and will provide you with more information as it becomes available. If you have any questions, please call the NIACC Business Office at 641-422-4214 or email Mindy.Eastman@niacc.edu.

[DATE]

[FIRST NAME, LAST NAME
ADDRESS
CITY/STATE/ZIP]

NOTICE OF DATA BREACH

Dear [FIRST NAME],

We greatly appreciate your commitment as a student at North Iowa Area Community College ("NIACC"). We respect and protect the privacy of your information, and we are writing to let you know about a data incident that involved unauthorized access to information about you that NIACC possesses, as detailed below.

WHAT HAPPENED?

On Tuesday, May 18, 2021, an unknown and unauthorized person impersonated a NIACC employee and sent a phishing email to another NIACC employee requesting student information. This phishing attack led to the compromise of two documents tied to student account balances and containing other information about you. Within 30 minutes after the data compromise, the NIACC employee determined he was a victim of a phishing attack and immediately reported the incident to NIACC Administration. NIACC Administration contacted the school's Chief Information Officer immediately.

WHAT INFORMATION WAS INVOLVED?

Out of an abundance of caution, we want to alert you that certain information contained in the compromised documents was exposed to the attacker. The compromised document contained the following information: name, address, student identification number, social security number, cell phone number, home phone number, and student account balance. No other information was contained in the compromised documents.

HOW DID NIACC RESPOND?

Immediately upon learning of this incident, NIACC began an investigation to determine the nature of the attack and what information, if any, could have been compromised. After determining the contents of the documents acquired by the attacker, NIACC promptly sent an email to the potentially affected students to alert them of the incident and instruct them only to pay tuition, housing fees, and student fees through the NIACC Business Office or through TrojanHome to protect themselves from potential financial crimes. NIACC also instructed all potentially affected students to not send money to anyone purporting to be collecting monies owed to NIACC over phone, text messages, or emails. NIACC also directed the potentially affected students to notify the NIACC Business Office if they experienced any suspicious activity related to their tuition

balances. NIACC also reported the incident to the local police department and the Federal Bureau of Investigation. Notification has not been delayed by law enforcement investigation.

WHAT CAN YOU DO?

NOTIFY LAW ENFORCEMENT OF SUSPICIOUS ACTIVITY AND CONTACT CONSUMER REPORTING AGENCIES

As a precautionary measure, we recommend that you remain vigilant, review account statements, monitor free credit reports, and report any suspicious activity or suspected incidence of identity theft to proper law enforcement authorities, including your state Attorney General's office and the Federal Trade Commission (FTC). You have the right to file or obtain a police report regarding the breach. You can obtain information from the FTC and the Consumer Reporting Agencies requesting fraud alerts and security freezes as explained below.

To report fraudulent activity with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Reports filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

We also recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at:

https://www.annualcreditreport.com/requestReport/requestForm.action.

Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http:// www.annualcreditreport.com.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed above.

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as J., Sr., II, III, etc.);
2. Social security number;
3. Date of birth;
4. If you have moved in the past 5 years, provide the addresses where you have lived over the prior 5 years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have 1 to 3 business days after receiving your request to place a security freeze on your credit file report, based upon the method of the request. The credit bureaus must also send written confirmation to you within 5 business days and provide you with the process by which you may remove the security freeze, including an authentication mechanism. Upon receiving a direct request from you to remove a security freeze and upon receiving proper identification from you, the consumer reporting agency shall remove a security freeze within 1 hour after receiving the request by telephone for removal or within 3 business days after receiving the request by mail for removal.

CONTACT THE NIACC BUSINESS OFFICE WITH ANY QUESTIONS RELATED TO TUITION

As we've already advised, NIACC recommends that students who have any questions related to their student accounts and tuition balances to contact the NIACC Business Office. Staff from the NIACC Business Office can assist students with paying tuition, housing fees, and student fees in a safe and secure manner.

WHAT WE ARE DOING

In addition to NIACC's already robust information security plan, NIACC took further remedial steps by emailing all faculty and staff with a summary of the incident and requiring additional cybersecurity training. NIACC Administration also held one-on-one discussions with faculty and staff to ensure they can identify future phishing emails.

NIACC will be strengthening its technical, organizational, and administrative controls and implementing policies and procedures to ensure requests for protected information are verified appropriately and no protected information is shared absent appropriate encryption.

Finally, we are offering identity theft protection services through ID Experts® to provide you with MyIDCare™. MyIDCare services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 1-800-939-4170 or going to https://app.idx.us/account-creation/protect and using the following Enrollment Code: [_____]. MyIDCare experts are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is October 10, 2021. We encourage you to take full advantage of this service offering. MyIDCare representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

FOR MORE INFORMATION

NIACC values your privacy and deeply regrets that this incident occurred. If you would like additional information, please contact:

Mindy Eastman, Comptroller – NIACC
NIACC Business Office
Phone: 641-422-4214
Email: Mindy.Eastman@niacc.edu

Sincerely,

[SIGNATURE]